

**UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF TENNESSEE  
NASHVILLE DISTRICT**

<b>UNITED STATES OF AMERICA</b>	)	
	)	
<b>v.</b>	)	<b>No. 3:13-00118</b>
	)	<b>Judge Sharp</b>
<b>MICHAEL MANCIL BROWN</b>	)	

**MEMORANDUM**

Defendant Michael Mancil Brown’s Motion to Suppress Evidence, which incorporates a request for a hearing pursuant to Franks v. Delaware, 438 U.S. 154 (1978), has seemingly taken on a life of its own. Ten briefs totaling more than 175 pages have been submitted, three of which were filed after this Court heard oral arguments on the motion, and the last of which was filed on October 15, 2014. For the reasons that follow, Defendant’s Motion will be denied.

**I. BACKGROUND**

On June 26, 2013, a federal grand jury returned a twelve-count Indictment against Defendant. The first six counts allege wire fraud in violation of 18 U.S.C. §§ 2 & 1343; the last six counts allege violations of 18 U.S.C. §§ 2 & 1952(a)(3) for using a facility of interstate commerce to carrying on an unlawful activity, specifically extortion. All concern an alleged scheme to defraud in relation to the threatened release of tax returns for 2012 Presidential Candidate Mitt Romney that were allegedly purloined from the computer system of accounting firm PricewaterhouseCoopers.

The Indictment followed the search of Defendant’s residence pursuant to a warrant. That warrant, signed by Magistrate Judge Griffin, was based upon a 36-page affidavit from Secret Service Agent Matt Stephenson. Because that warrant is at the center of the pending Motion, the Court discusses it in some detail. Except where otherwise noted, the following is drawn from the affidavit.

Fully half of the warrant affidavit deals with a prior investigation of Defendant by the Secret Service. The events leading to the investigation began on October 27, 2009, when a local television reporter contacted “Insurance Company A,” and told the company that he had been contacted by a man named Michael Brown who said he was in possession of the insurance company’s customer data. The reporter also allegedly reported that Brown claimed to be a “Good Samaritan” who was trying to inform the company of certain vulnerabilities in its computer system and went to the media after the company ignored his entreaties about the problem.

That same day, Brown allegedly phoned an employee in the public relations section of the insurance company and told him that he had obtained access to customer information through a vulnerability in the computer system and that he had a database of information for approximately 2,000 customer, including their social security numbers. That call was followed by an e-mail from the address “Michaels<kinghtmb@kighttmb.dyndns.org>”, which attached a Microsoft Excel spreadsheet containing 2,200 rows of customer data. The accompanying text was signed, “Thanks, Michael.”

On November 2, 2009, the head of information technology for Insurance Company A spoke with Brown about how he had come into possession of the data and was informed that, while assisting an Insurance Company A employee named “Liz” with a computer problem at the Sommet Center, he (Brown) discovered that access could be gained to the customer database by copying a webpage address for Insurance Company A from Liz’s computer and then pasting that address into the web browser of his own computer. Brown stated that he had attempted to contact Insurance Company A about the problem, but, when he received no response, he contacted the local news media.

By early November 2009, the Secret Service had been brought into the matter. On November 3, 2009, outside legal counsel for Insurance Company A informed Secret Service Agent Lee Eaves that a database of information given to the company by Brown contained the names and addresses of approximately 2,100 customers, that Brown said he got the information off of Liz's computer, that Insurance Company A could identify no such named employee at the Sommet Center, that Brown had previously been an Insurance Company A customer and his agent was Insurance Agent B, and that Insurance Agent B had resigned from the company after he was confronted with alleged wrongdoing. Counsel also told Agent Eaves that there were an inordinate amount of transactions relating to Agent B's account through Internet Protocol ("IP") address 75.146.8.201.

That same day, Agent Eaves learned the IP address was assigned to Endless Sphere Technologies at 107 Cadet Circle, Franklin, Tennessee, which (Agent Eaves later learned) was Defendant's residence. He also discovered that Endless Sphere was Brown's company and that it claimed to provide wireless internet services, including web and e-mail hosting.

The following day, Agent Eaves contacted the Franklin Police Department to learn if it had received any complaints about Brown. He was informed that a complaint had been made by Brown's ex-girlfriend, alleging Brown had accessed her bank account and transferred \$500 to a PayPal account.

Agent Eaves secured a search warrant for Brown's residence. The warrant was executed on November 18, 2009, at which time Agent Eaves interviewed Brown. Brown stated that in April or May 2009, he had been approached by Agent B who said that he was leaving Insurance Company A and wanted the list of Insurance Company A's customers so that he could use it to call on them

when he moved to another insurance company. Brown later agreed to download the list for \$400. Utilizing Agent B's username and password, Brown downloaded the information on his personal computer at his residence.

Brown continued by stating that, in the latter part of July 2009, he gave Agent B the list (stored on a compact disc), but was only given \$250, instead of \$400 as agreed. Sometime later, Brown saw a news story about an individual being arrested for unauthorized access to a computer system and he became concerned that he could be held criminally liable. Brown claimed that he tried to contact Insurance Company A on numerous occasions to tell them what happened, but received no response. It was then that he contacted a television news reporter, giving the reporter a false description of how he had come into possession of the customer list.

Brown went on to say that he kept the customer records from Insurance Company A in a folder on his personal computer. He claimed, however, that he had removed the social security numbers from the data and retained only the names, addresses, and telephone numbers of the customers.

At Agent Eaves' request, Brown met with Agent B on two separate occasions. Both times, Brown wore a wire. Both times, Insurance Agent B made incriminating statements.

Forensic examinations of Brown's personal computer and the CD he had given to Insurance Agent B (but subsequently retrieved) revealed four Microsoft Excel spreadsheet files containing far more than the claimed 2,000 names, addresses and telephone numbers. The "Belle Meade-Forest Hills" file contained approximately 1,800 listings; the "Bellevue" file approximately 2,100; the "Brentwood" file approximately 5,000 listing; and the "Franklin" file approximately 8,700.

After a search of Insurance Agent B's office, he was interviewed by Agent Eaves. Insurance

Agent B admitted that he hired Brown to access Insurance Company A's computer system in order to obtain customer information, and provided Brown with his user name and password. He said he intended to use the information so that he could market his new position with another insurance company to his former customers.

On January 13, 2012,<sup>1</sup> Brown was administered a polygraph examination during which he confirmed that he had been hired by Insurance Agent B to retrieve Insurance Company A client information. Brown further stated that he was able to retrieve the social security numbers of the customers, but did not provide those numbers to Insurance Agent B (as he had previously claimed) and did not retain those numbers himself. Brown then refused any further requests for interviews.

In the warrant affidavit in this case, Agent Stephenson opines that, at the conclusion of the 2009 investigation, it appeared that Brown had falsely told Insurance Company A that he had obtained social security numbers and access to the customer database through a vulnerability in the computer system. Agent Stephenson also opined that it appeared Brown may have been motivated by the hope that Insurance Company A would hire him to provide computer security consulting services and that the publicity generated by the television report might bring him computer security consulting business from other sources.

Turning to the present charges, the warrant affidavit states that on August 28, 2012, a suspicious package was found in PricewaterhouseCoopers' mail in Franklin, Tennessee. That package contained a thumb drive, and a letter bearing a scanned signature for "Mitt Romney." The letter, which was attached as an exhibit to the warrant affidavit suggested that the thumb drive contained encrypted copies of tax documents for "Willard M[.] Romney and Anne D[.] Romney."

---

<sup>1</sup> The Court italicizes the date because it is incorrect. The actual date was January 13, 2010.

The letter stated that access had been gained to PricewaterhouseCoopers' network file servers and that the Romney's tax files had been copied. It further stated that the major news organizations were going to be sent encrypted copies of the couple's return for the most recent tax years. If, however, "interested parties" did not want the encryption key to unlock the documents released on September 28, 2012, payment of \$1,000,000 worth of Bitcoins<sup>2</sup> would have to be transferred to the "Stop Release" Bitcoin address. On the other hand, those who wanted the encryption key "made available to the world right away" would be instructed to send \$1,000,000 in Bitcoins to a "Promote Full Release" address.

On August 30, 2012, the Secret Service was told about the suspicious package and, the following day, examined the thumb drive. That drive contained an encrypted file named "ROMNEY1040-Collection.7z,"<sup>3</sup> which Agent Stephenson stated the Secret Service had been unable to decrypt. There was also unallocated space that contained the words "dolphin" and "Kathryn."

On September 1, 2012, PricewaterhouseCoopers informed agents that an internal investigation showed no evidence that its servers had been compromised and no indication that the Romney's tax information had been transferred. Further, a review of logs of employees who had access to the documents showed no unusual patterns.

The following day, a description of the alleged theft of the tax information was posted to

---

<sup>2</sup> "Bitcoin is the name of an encrypted online currency. It is managed through a private network and not through any Government, central bank or formal financial institution." United States v. Ulbricht, 2014 WL 5090039, at \*1, n.1 (S.D.N.Y. Oct. 10, 2014).

<sup>3</sup> "A file with the .7z extension is a compressed file generated by file archive software called 7-Zip (see [www.7-zip.org](http://www.7-zip.org)). A .7z file can contain multiple files and folders all compressed into the single .7z file." Apantac, LLC v. Avitech Int'l Corp., 2014 WL 3105006, at \*3, n.5 (D. Or. June 24, 2014).

<http://pastebin.com/zdU1TK40>,<sup>4</sup> and a copy of that posting was attached to the warrant affidavit. The message described the alleged theft of the tax records, and indicated that similar packages had been delivered to the offices of the Democratic Party and the Republican Party in Williamson County, Tennessee. Two days later, the letter sent to PricewaterhouseCoopers was posted on Pastebin.

The first Pastebin message was posted from IP address 31.172.30.1, which was assigned to Chaos Computer Club e.V in Hamburg, Germany. That club provides anonymous network services and provides a Tor exit-node to the end user.<sup>5</sup> The second was made from IP address 199.48.147.45, which was assigned to Formless Networking LLC in San Francisco, California, and was the Tor exit router, *i.e.*, the last computer in the Tor relay system before it reaches its intended destination.

On September 4, 2012, the Pastebin posts were quoted in a blog post by the local CITY PAPER and later picked up by numerous media outlets around the United States. The following day, agents obtained the thumb drives that had been in the packages delivered to the Franklin County Democratic and Republican Party offices. Much of the information on the thumb drives was the same as that found on the thumb drive delivered to PricewaterhouseCoopers. However, the one mailed to the Republican Party contained two pictures of cats on the unallocated space. The word

---

<sup>4</sup> Pastebin.com is a website where text can be stored online for a specified period of time.

<sup>5</sup> Tor is an acronym for “The Onion Router.” The “TOR Project” has been described as follows:

In a nutshell, the Tor Project functions by rerouting a user’s online activity through an international network of servers, allowing the user to reach an online destination through one of many “exit nodes.” The user’s destination site then records the exit node’s IP address rather than the user’s true IP address, making it very difficult to trace the user’s true identity. The Tor Project does not disclose the IP addresses of its exit nodes[.]”

F.T.C. v. Asia Pacific Telecom, Inc., 788 F. Supp.2d 779, 786-87 (N.D. Ill. 2011).

“dolphin” in the test string “4154 dolphin KnightMB” was found multiple time in the unallocated space on the thumb drive delivered to the Democratic Party.

A web search for “KnightMB” ultimately linked to a blog entry that contained references to Tennessee, Bitcoin.org, and the name “Michael Brown” with the nickname of “KnightMB.” A link on the blog led to the discovery that KnightMB lived in Franklin, Tennessee, and was thirty-three years old. The warrant affidavit describes in detail at least seven ways in which “KnightMB” is linked to Michael Brown, the Defendant herein, including that it was used on the email sent to the public relations department at Insurance Company A. Additionally, an internal inquiry indicated that a likely relative of the Defendant was “Kathryn” Thomas, and a popular file manager system of the Linux operating system which KnightMB used is named “Dolphin.” A Secret Service Agent who had been involved in the prior investigation recognized the name, address and driver’s license photograph of Brown.

On September 8, 2012, another post was made to Pastebin, this time signed “Dr. Evil.” That post addressed some of the questions raised by recent news articles and directed readers to documents on a webpage on 4shared.com, a web hosting site. An encrypted document titled “Romney1040-Collection,” containing the same hash value as the encrypted documents found on two of the three thumb drives, was posted on the webpage. In answer to one of the questions that had been raised, Dr. Evil wrote “Our only advise [sic] to the Republican office is to get a mail-slot like the Democratic office had[.]” The October 27, 2009, e-mail to Insurance Company A also improperly used “advise” when the word “advice” was proper.

On September 11, 2012, Secret Service Agent Kelvin Jackson posed as a utility worker near Brown’s residence, which by then was confirmed to be 107 Cadet Circle in Franklin. At one point,



Brown exited the residence, approached the surveillance vehicle, and remarked that he had been meaning to contact the utility because the light on the pole flickered. That same day, an IP pen register (authorized by court order) indicated that at 9:05:34 a.m., the static IP address assigned to 107 Cadet Circle connected to IP address 31.172.30.1, the same IP address for Chaos Computer and the Tor exit node attributed to the first Pastebin post.

The warrant affidavit suggested similarity between the 2009 investigation of Brown and the present investigation. Agent Stephenson wrote:

The 2009 investigation of Brown is similar to the current investigation in that Brown falsely claimed to have gained unauthorized access to the computer systems of a large corporate entity and falsely claimed that he had obtained highly sensitive customer information. In the current investigation, the individual making similar claims has maintained his anonymity. This may be the result of the law enforcement response to Brown's claims when he identified himself to the news media and to the representatives of "Insurance Company A" in 2009.

(Docket No. 4, Warrant Aff. at 27 ¶ 31).

## **II. SUMMARY OF DEFENDANT'S ARGUMENTS**

In his initial filing, Defendant identified one false statement and several omissions that he claims distorted the facts before Magistrate Judge Griffin. Defendant contends that, had the information been presented properly, no warrant would have issued.

More specifically, he asserts that the warrant affidavit was plainly false when it claimed Brown's polygraph was in 2012, instead of 2010, and this error gave the false impression that the investigation was not only ongoing, but also that Brown was lying about having obtained customer's social security numbers. Not only did he pass the polygraph examination,<sup>6</sup> the Secret Service

---

<sup>6</sup> During the polygraph examination, Defendant conceded that he downloaded items that had social security numbers but claimed that he had destroyed any data containing such information and did not have in his possession any social security numbers. The examiner concluded that Defendant showed "no deception."

actually asked Brown to sign a hold harmless waiver in relation to the 2009-2010 investigation.<sup>7</sup>

As for omissions, Defendant claims that they “pertain to virtually every fact that the affidavit made to draw suspicion to [him].” (Docket No. 26 at 12). His initial filing, however, points to only three: (1) the affidavit stated that two text strings on the thumb drives pointed to Defendant, but the affidavit neglects to state that the picture of a cat on one of those thumb drives shows a cat that is not at Defendant’s house; (2) the affidavit indicates that Defendant is very computer savvy, familiar with Bitcoin, and can use 7-zip, yet fails to point out that, due to his involvement in a computer business, his IP addresses serve any of a number of internet users; and (3) the affidavit states that Defendant spelled “advice” with an “s,” but neglects to point out that in another writing he spelled “advice” properly.

With virtually every filing, Defendant has identified either additional omissions and/or amplified the arguments he made in relation to those previously identified. In his initial Reply Brief, Defendant asserts that the entire 2009-2010 incident was blown out of proportion. He argues:

Brown was a Good Samaritan turned whistleblower. He had found what he considered a two-fold flaw in Company A’s website. First, it was a flaw that any given agent could access a vast number of customer social security numbers. Second, it was a flaw that this access could be made by using the URL shown upon accessing the agent page with the agent’s username and password. Because he viewed those aspects of Company A’s website as flaws, he tried to notify Company A. As a Good Samaritan, he tried to do so discreetly. When Company A irresponsibly ignored his efforts, he blew the whistle.

(Docket No. 43 at 4). Defendant also contends that Agent Stephenson exaggerated the significance of the Tor connection by leaving the impression that at 9:05 on September 11, 2012, Defendant connected with Tor using the same node used by the Pastebin poster when, in fact, “Mr. Brown or

---

<sup>7</sup> Apparently, the hold-harmless waiver was a part of a consent to delete data agreement that was required prior to the return of Defendant’s computer equipment in 2010.

one of his many customers of which there were possibly more than 150, connected with Tor” at that time. (Docket No. 43 at 6).<sup>8</sup>

In his Supplemental Brief Defendant claims that, with respect to the 2009-2010 investigation, “[t]he warrant affidavit created misimpressions through falsehood, false implication, and material omission,” in the following particulars:

- (1) The affidavit created the false impression that Brown involved the media in the matter needlessly and wantonly;
- (2) It created the false impression that there was no security problem to report; and
- (3) It created the false impression that the investigation culminated recently (in that same year, 2012) with a polygraph catching Brown in a lie.

(Docket No. 73 at 1).

Defendant’s arguments are not limited to the search warrant affidavit presented to Magistrate Judge Griffin. In his Reply to the Government’s Response to his Supplemental Brief, Defendant argues that, in the “affidavit for the warrant to conduct the IP pen register, the affiant swore that ‘Michael Brown was previously investigated by federal criminal authorities for *threatening to expose* a company’s vulnerabilities *if he was not given a job*.” (Docket No. 77 at 2, emphasis added by Defendant).<sup>9</sup> While Defendant acknowledges that the affiant goes on to opine that “a possible rational motive for [Defendant’s] conduct was that he hoped for security consulting work,” he argues this is “nothing but off-base speculation, and thus it was wrong to convey this speculation to the

---

<sup>8</sup> According to Defendant, he has an 85' tower at his residence, a tower that would have been obvious to investigating officers.

<sup>9</sup> Technically, this was an Application made by the Assistant United States Attorney pursuant to 18 U.S.C. § 3122(b) which requires “certification by the applicant that the information likely to be obtained [from a pen register and trap and trace device] is relevant to an ongoing criminal investigation being conducted by that agency.”

judge as if it were known fact.” Id.

### **III. FRAMEWORK FOR ANALYSIS**

In Franks, the United States Supreme Court recognized a “defendant’s right to challenge the sufficiency of an executed search warrant by attacking the veracity of the affidavit supporting the warrant,” and “granted defendants a limited right to an evidentiary hearing concerning the veracity of the affidavit.” United States v. Fowler, 535 F.3d 408, 415 (6<sup>th</sup> Cir. 2008). “[W]here the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.” Franks v. Delaware, 438 U.S. 154, 155–56 (1978).<sup>10</sup> Thus, “[a] defendant is entitled to a Franks hearing if he: 1) makes a substantial preliminary showing that the affiant knowingly and intentionally, or with reckless disregard for the truth, included a false statement or material omission in the affidavit; and 2) proves that the false statement or material omission is necessary to the probable cause finding in the affidavit.” United States v. Rose, 714 F.3d 362, 370 (6<sup>th</sup> Cir. 2013) (citing Franks, 438 U.S. at 171–72).

Both prongs must be satisfied before a hearing is required. “Therefore, ‘if, when material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause, no hearing is required.’” United States v. Mastromatteo, 538 F.3d 535, 545 (6<sup>th</sup> Cir. 2008) (quoting Franks, 438 U.S. at 171–72). If, however, “both prongs are satisfied and at the evidentiary hearing, ‘the

---

<sup>10</sup> This showing must be “accompanied by an offer of proof. . . . Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained[.]” Id. at 171.

allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search' suppressed.'" United States v. Graham, 275 F.3d 490, 505 (6<sup>th</sup> Cir. 2011) (quoting Franks, 438 U.S. at 156).

False statements or misrepresentations can be an act of commission or omission. See United States v. Carpenter, 360 F.3d 591, 596 (6<sup>th</sup> Cir. 2004) (citation omitted) ("this court has recognized that 'material omissions [from an affidavit] are not immune from inquiry under Franks.'"). With regard to the latter, the Sixth Circuit "has repeatedly held that there is a higher bar for obtaining a Franks hearing." Fowler, 535 F.3d at 415.

"Allegations of material omission are held to a higher standard because of the 'potential for endless rounds of Franks hearings' due to potentially 'endless conjecture about investigative leads, fragments of information, or other matter that might, if included, have redounded to defendant's benefit.'" Id. at 415-16 (quoting United States v. Martin, 920 F.2d 393, 398 (6<sup>th</sup> Cir. 1990)). "[T]o be constitutionally problematic, the material must have been deliberately or recklessly omitted and must have *undermined* the showing of probable cause." United States v. Duval, 742 F.3d 246, 251 (6<sup>th</sup> Cir. 2013) (emphasis in original) (citing Carpenter, 360 F.3d at 596-97). "In the case of alleged material omissions – analogy to the standard for included false statements – the defendant is entitled to a hearing if and only if: (1) the defendant makes a substantial preliminary showing that the affiant engaged in deliberate falsehood or reckless disregard for the truth in omitting information from the affidavit, and (2) a finding of probable cause would not be supported by the affidavit if the omitted material were considered to be a part of it." Fowler, 535 F.3d at 415.

### III. ANALYSIS

Although Defendant's "Good Samaritan" self-characterization seems a bit much, and notwithstanding that a defendant seeking a Franks hearing "has a heavy burden," United States v. Bennett, 905 F.2d 931, 934 (6th Cir. 1990) – particularly if the request is based on alleged material omissions – one could conclude that he has made a substantial preliminary showing that the warrant affidavit was drafted with reckless disregard for the truth, even if that was not Agent Stephenson's intention. Maybe the date of the polygraph was a mere scrivener's error, but that mistake could leave the impression that the 2009-2010 investigation was still-ongoing.<sup>11</sup> One could also conclude that the investigation was not favorable to Defendant because the warrant affidavit omitted any mention that Defendant was deemed to have not been deceptive during relevant portions of the polygraph examination and was asked to sign a hold-harmless waiver, both of which could suggest the investigation was going, or went, nowhere. Add to that the pictures of the cats in the window of a residence, something which seems totally innocuous, but could lead a reader to conclude that they were Defendants' cats, linking him to the thumb drive found at the Republican Party Headquarters. And there is the absence of any suggestion of the number of Internet customers Defendant allegedly had which could suggest that any of a number of individuals could have been using the Internet when access was made to IP address 31.172.30.1 from 107 Cadet Circle on September 11, 2012. The Court recognizes that in support of its position that no Franks hearing is necessary, the Government presented a 21-page affidavit in which Agent Stephenson acknowledges what he claims to be a mere scrivener's error in the date of the polygraph exam, notes a couple of

---

<sup>11</sup> Actually, it appears unlikely that Magistrate Judge Griffin was misled into concluding that the investigation was still ongoing. After misstating the date of the polygraph examination, Agent Stephenson began the very next paragraph by writing "[a]t the conclusion of the 2009 investigation of Michael Brown . . . ." (Docket No. 4, Stephenson Aff. p. 26).

more errors,<sup>12</sup> and addresses the three alleged omissions identified by Defendant in his opening brief.

Agent Stephenson avers that while he was aware that the cat picture on the Republican Party thumb drive appeared to have been taken at a location other than Defendant's residence, he "did not believe that it added to or diminished the probable cause for a search" and the "fact that the image did not appear to be taken at [Defendant's] then current residence did not mean that the image had no connection" to him. (Docket No. 30-1, Stephenson Aff. ¶¶ 55 & 57). As for Defendant's claim that he had at least 150 customers, Agent Stephenson states that he (1) was aware that Defendant claimed to provide Internet service to individuals living nearby; (2) did not know how many customers Defendant claimed to have, but believed that only five households in the vicinity may have been using Defendant's internet address; and (3) does "not believe that the number of customers that defendant Brown's wireless Internet service claimed to serve would have diminished the probable cause to search his residence." (Id. ¶ 62).

With regard to the assertion that Defendant correctly used the word "advice" (instead of "advise"), Agent Stephenson acknowledges that the document with the proper usage was in records of the Secret Service at the time the warrant was sought, but that he personally was unaware of it and, in any event, does not believe that the fact that the word was used correctly "on one occasion neglected the fact that he also at times misused the word[.]" (Id. ¶ 68). Finally, with regard to all three omissions, Agent Stephenson claims that those facts were not "omitted . . . deliberately, knowingly, intentionally or in reckless disregard for the truth," and he does not believe that the

---

<sup>12</sup> Two of those errors corrected statements that indicated Agent Stephenson was told something when in fact Agent Eaves was the recipient of the information.

“omitted facts, even if true, diminished the probable cause for a search of defendant Brown’s residence.” (Id. ¶ 69).

The Court does not place a great deal of weight on that affidavit because Agent Stephenson’s credibility has not been subjected to scrutiny, and reliance on an affidavit in lieu of a hearing may be error. See, United States v. McMurtrey, 794 F.3d 502, 504 (7<sup>th</sup> Cir. 2013) (in considering whether a full-Franks hearing is warranted, “the natural temptation for the court will be to invite and consider a response from the government. However, the court should not give the government an opportunity to present its evidence on the validity of the warrant without converting the hearing into a full evidentiary Franks hearing, including full cross-examination of government witnesses.”). Moreover, whether something added to, or detracted from, the determination of probable cause was for the Magistrate Judge to make:

The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. . . . The right of officers to thrust themselves into a home is . . . a grave concern, not only to the individual but to a society which chooses to dwell in reasonable security and freedom from surveillance. When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.

Johnson v. United States, 333 U.S. 10, 13-14 (1948) .<sup>13</sup>

But whether Defendant has actually made the substantial preliminary showing, and whether the Government has provided plausible reasons for what are principally omissions in the warrant

---

<sup>13</sup> To be clear, and to alleviate the concern raised by the Government in its last filing, the Court is not stating that an officer should not present the Magistrate Judge with the inferences he (the officer) draws from what was learned in the investigation. What the Court is stating is that the determination of probable cause is ultimately for the Magistrate Judge to make, not the investigating officer.



affidavit, need not be definitively resolved by the Court. This is because when the allegedly false statements are removed and the alleged omissions are included, there was more than enough to establish probable cause.

“‘The test for probable cause is simply whether there is a fair probability that contraband or evidence of a crime will be found in a particular place.’” United States v. Miller, 314 F.3d 265, 268 (6<sup>th</sup> Cir. 2002) (quoting United States v. Murphy, 241 F.3d 447, 457 (6<sup>th</sup> Cir. 2001)). “In other words, a magistrate need only find ‘reasonable grounds for belief’ that evidence will be found in order to justify the issuance of a search warrant.” United State v. Thomas 605 F.3d 300, 307 (6<sup>th</sup> Cir. 2010) (citing United States v. Bennett, 905 F.2d 931, 934 (6<sup>th</sup> Cir.1990)). Stated yet another way, “‘the issuing magistrate must have reasonable grounds for belief, supported by less than prima facie proof but more than mere suspicion,’ United States v. Coffee, 434 F.3d 887, 892 (6<sup>th</sup> Cir. 2006) (internal quotation marks omitted), that ‘a nexus [exists] between the place to be searched and the evidence sought,’ United States v. Carpenter, 360 F.3d 591, 594 (6<sup>th</sup> Cir.2004) (en banc) (internal quotation marks omitted).” United States v. Neal, 577 F. App’x 434, 437 (6<sup>th</sup> Cir. 2014). Moreover, “[s]earch warrant affidavits are to be judged on the totality of the circumstances, not line-by-line scrutiny.” Thomas, 605 F.3d 307; see also United States v. Allen, 211 F.3d 970, 975 (6<sup>th</sup> Cir. 2000) (“The affidavit is judged on the adequacy of what it does contain, not on what it lacks, or on what a critic might say should have been added.”).

It is undisputed that Defendant accessed Insurance Company A’s computer database and downloaded customer information for pecuniary gain. It is also undisputed that Defendant initially lied about how he accessed the information, and claimed that he had accessed social security numbers. It is further undisputed that Defendant ultimately went to the media, even if he claims

that he did so to expose a supposed vulnerability. Similarly, and also in the same geographic area, PricewaterhouseCoopers was contacted by an individual who claimed to have gained unauthorized access to its computer system, thereby obtaining sensitive and confidential information. And just as in the Insurance Company A incident, the media was contacted.

Apparent similarities between the two investigations aside, there was abundant information from which Magistrate Judge Griffin could find probable cause, even adding the facts which Defendant claims were omitted and correcting the date for the polygraph examination. The fact that a thumb drive had pictures of cats which were not as yet linked Defendant<sup>14</sup> does not negate the fact the word “KnightMB” was found on the thumb drive obtained from the offices of the Democratic Party, or that the word “Kathryn” was on the thumb drive obtained from the offices of PricewaterhouseCoopers. It also does not negate the fact that Defendant had been linked to both, and to “KnightMB” in many ways. Nor did it negate the fact that the username “KnightMB” was linked to Bitcoin and the use of 7-Zip encryption software.

Further, none of the foregoing is diminished by the fact that Defendant may have used the word “advise” correctly on occasion. In the October 27, 2009 e-mail to Insurance Company A, Defendant improperly used “advise” when “advice” was proper, just as the author of the “Dr. Evil” letter confused the words. The fact that Defendant did not always make that mistake does not cancel out the fact that he sometimes made that mistake.

Moreover, none of the foregoing is diminished by the fact that Defendant claims many individuals used his IP address. While it is possible that one of Defendant’s alleged customers could

---

<sup>14</sup> After the search warrant was executed, Defendant was allegedly linked to the photos because they were on a neighbor’s computer that Defendant had repaired.

have accessed the Tor exit node on September 11, 2012, it was just as likely that Defendant did so, particularly given all the other things that had been discovered during the investigation.

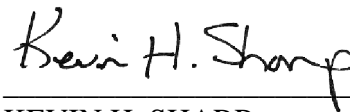
Finally, none of the foregoing is negated by the fact that the warrant affidavit provided the incorrect date for the polygraph exam, omitted to state that Defendant had been found not to be deceptive with regard to pertinent question, and neglected to state that Defendant was asked to signed a hold harmless waiver. The fact remains that the original investigation occurred and Defendant was at the center of it.

The Court could go on, but the issue is not whether the warrant affidavit (with the alleged falsity omitted and the alleged material omissions included) established beyond a reasonable doubt that evidence of a crime relating to the PricewaterhouseCoopers investigation would be found at 107 Cadet Circle. Rather, the question is whether the warrant affidavit, as revised, established a fair probability that contraband or evidence of a crime relating to that investigation would be found at Defendant's residence. It did.

## **V. CONCLUSION**

On the basis of the foregoing, Defendant's Motion to Suppress and incorporated request for a Franks hearing will be denied.

It is SO ORDERED.



---

KEVIN H. SHARP  
UNITED STATES DISTRICT JUDGE